(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 October 2001 (04.10.2001)

PCT

(10) International Publication Number
WO 01/74003 A1

(51) International Patent Classification[7]: H04L 9/00, H04H 1/02

(21) International Application Number: PCT/US01/09797

(22) International Filing Date: 27 March 2001 (27.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/538,373 29 March 2000 (29.03.2000) US

(71) Applicant: SONY ELECTRONICS, INC. [US/US]; 1 Sony Drive, Park Ridge, NJ 07656 (US).

(72) Inventors: MARUO, Jun; Tomigaya, Shibuya-Ku, Tokyo 1-88-15-303 (JP). KAGAMI, Atsushi; Ru # 402, Komagome, Toshima-Ku, Tokyo 4-12-10 (JP).

(74) Agents: GALLENSON, Mavis et al.; Ladas & Parry, 5670 Wilshire Blvd., Suite 2100, Los Angeles, CA 90036 (US).

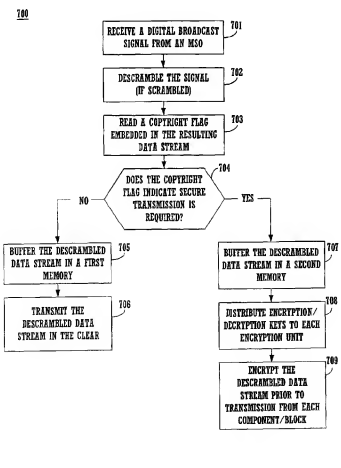
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

[Continued on next page]

(54) Title: TRANSCEIVER SYSTEM AND METHOD



(57) Abstract: A system for selectively implementing secure transmission of data between internal components of the transceiver (FIG.3A). The transceiver includes a first component for receiving data stream from an external source. A first encryption unit is coupled to the first component for encrypting the data stream to produce an encrypted data stream. The transceiver also includes a second component coupled to the first component via a bus to receive the encrypted data stream. A second encryption unit is coupled to the second component for decrypting the encrypted data stream. As the data stream is received by the transceiver from the external source, the first encryption unit is configured to read a flag included in the data stream that indicates whether the data stream requires secure transmission. When the flag (FIG.7, #704) indicates secure transmission is required, the first encryption unit encrypts (FIG.7, #709) the data stream and transmits via the bus the resulting encrypted data stream to the second component for further processing. When the flag indicates secure transmission is not required, the data stream is transmitted via the bus to the second component without encryption (FIG. 7, #706).

WO 01/74003 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TRANSCEIVER SYSTEM AND METHOD

FIELD

The present disclosure relates to the field of intelligent transceivers such as bi-directional set-top boxes used by the cable television industry. Specifically, the present disclosure pertains to a method and system for selective encryption of data signals on a data bus in a transceiver. More specifically, the present disclosure pertains to a method and system for maintaining secure transmission of copyrighted data between internal components of an intelligent transceiver while reducing overhead required for the secure transmission process.

BACKGROUND ART

Digital broadcast systems include direct broadcast digital satellite systems, interactive World Wide Web ("Web") access systems, and digital cable systems. Digital broadcasting provides a number of advantages to subscribers, such as variety and flexibility of programming, useful and comprehensive support services (such as detailed electronic programming guides), and superior audio and video quality.

The Conditional Access (CA) function of a digital broadcast system allows selective access to valuable copyrighted information. Such information includes, for example, pay-per view movies, premium sporting events, etc. The

producers of the movies, events, etc., require that access to the premium services be controlled in order to protect and enforce their copyrights, protect copyright ownership, and protect their commercial interests as well. The digital broadcast system operators (also referred to as Multiple System Operators, MSOs) also have a commercial interest in limiting access to these copyrighted premium services to authorized users only.

Subscribers receive digital broadcasts (including satellite, cable and Web broadcasts) via set-top boxes or other similar consumer electronic equipment located in the subscriber's home. With a bi-directional set-top box, in addition to receiving broadcasts, a subscriber can transmit messages to the MSO. Using the bi-directional set-top box (generally, a "transceiver" or "intelligent transceiver"), the subscriber selects a premium service, and the subscriber's selection as well as information needed for billing purposes is transmitted to the MSO. For example, in a common implementation, a "smart card" stores the information needed for billing, and on a periodic basis (perhaps once per month) an automatic connection is made between the transceiver and the MSO so that the billing information can be transmitted to the MSO.

Digital broadcast content is vulnerable to unauthorized use and duplication ("pirating") while it is being broadcast, or after it has been received and is being processed in the electronic device. For example, during broadcast, the signal could be intercepted and displayed (or duplicated and rebroadcast) using a transceiver not provided by the MSO. On the other hand, even when a transceiver provided by the MSO is used, the signal could be diverted within the transceiver so that the smart card is bypassed. In either case, copyrights are

circumvented. In addition, the MSO is unaware of the unauthorized use and so does not have the information needed to collect the fees it is owed.

To prevent unauthorized use, MSOs typically broadcast a scrambled signal. The scrambled signal is then descrambled by a descrambling unit in the transceiver (e.g., using a key provided by the MSO, for example, in the smart card). However, the typical transceiver includes a number of internal components or functional blocks. To provide the copyrighted services to the user, the descrambed signal needs to be coupled to one or more additional internal components of the transceiver for further processing. To prevent pirating of the descrambled signal, certain secure transmission techniques use encryption and decryption to protect the descrambled signal as it is transmitted among the internal components, for example, along one or more internal busses. Thus, the descrambled signal is not exposed "in the clear" as it is transmitted between the internal components to thwart the pirates.

Prior Art Figure 1 is a block diagram showing some of the elements in one transceiver (e.g., a set-top box). It should be noted that for clarity, not all of the elements of the set-top box are shown. Front-end unit 20 of the set-top box comprises a tuner (not shown), as well as other devices known in the art, for receiving a digital broadcast signal 90. Coupled to front-end unit 20 is a point of deployment (POD) 10. POD 10 typically is adapted to receive a smart card (not shown) that, as described above, can be used to provide billing information to the MSO. The smart card also typically contains a key provided by the MSO that is used to descramble digital broadcast signal 90. POD 10 includes a descrambling/encryption unit 40 that uses the key provided by the MSO to descramble broadcast signal 90 (if the signal is scrambled).

Descrambling/ encryption unit 40 also encrypts the signal (if the signal is not encrypted). It is appreciated that, in other prior art embodiments, descrambling functionality and the encryption functionality of unit 40 may consist of separate elements, one for descrambling and one for encrypting.

Front-end unit 20 also includes decryption unit 50 for decrypting an encrypted broadcast signal before the signal is sent to audio/visual (A/V) decoder 30. A/V decoder 30 is used for demultiplexing the signal and for decoding, for example, MPEG (Moving Picture Experts Group) video signals and/or Dolby AC3 audio signals.

Thus, in this embodiment, digital broadcast signal 90 is received by the set-top box at front-end unit 20 and forwarded to POD 10. Broadcast signal 90 is descrambled by descrambling/encryption unit 40. Once descrambled, broadcast signal 90 is encrypted to prevent unauthorized duplication. Further downstream in the set-top box, broadcast signal 90 is decrypted using decryption unit 50 so that it can be decoded (e.g., MPEG or AC3 decoding) in A/V decoder 30, and subsequently processed so that it can be viewed and/or listened to by an authorized subscriber.

A problem with this embodiment is that, between decryption unit 50 and A/V decoder 30, broadcast signal 90 is transmitted in the clear at point 12 (that is, it is not scrambled nor is it encrypted at this point). Thus, at point 12, broadcast signal 90 can be intercepted and duplicated. As a digital signal, it is possible to make near perfect copies which can be readily distributed to unauthorized parties (e.g., rebroadcast via the Internet, copied onto a compact disk, etc.). While the MSO may receive payment for a one-time use,

subsequent use by unauthorized users is made without proper compensation to the MSO or the copyright owners.

Prior Art Figure 2 illustrates some of the elements in another embodiment of a set-top box (for clarity, not all of the elements are shown). Front-end unit 20, descrambling/encryption unit 40, POD 10, decryption unit 50, and A/V decoder 30 each function in a manner as described above in conjunction with Figure 1. In this embodiment, an additional encryption unit 55 is included in front end unit 20 and a corresponding decryption unit is included in A/V decoder 30. Hence, in this embodiment, broadcast signal 90 is again encrypted (by encryption unit 55) before transmission across bus 57 to A/V decoder 30. A/V decoder 30 then decrypts broadcast signal 90 using decryption unit 56.

A problem with the embodiment of Figure 2 is that multiple encryption and decryption units need to be coordinated and operated. There exists a significant amount of overhead involved in maintaining the encrypt-decrypt processing of broadcast signal 90. For example, in one embodiment, multiple encryption/decryption keys need to be distributed and controlled among the various encryption and decryption units (e.g., units 40, 50, 55 and 56). This overhead imposes a significant processing penalty on the components of the set-top box. The overhead penalty is also imposed on the set top box embodiment of Figure 1.

SUMMARY

Accordingly, what is needed is a method and system that can prevent pirating of a descrambled and decrypted digital signal between multiple components (e.g., functional blocks) of an audio/video transceiver. What is also needed is a method and system to prevent pirating that can be implemented in a transceiver (e.g., a set-top box) used in a digital broadcast system. What is further needed is a method and system to prevent pirating that also reduces the overhead involved in managing an encryption/decryption process within a transceiver.

The present invention includes a method and system that satisfies the above needs. These and other advantages of the present invention not specifically mentioned above will become clear within discussions of the present invention presented herein.

In one embodiment, the present invention is implemented as a system for selective encryption of data as the data is transmitted between internal components of a transceiver. The selective encryption provides for a system for selectively implementing secure transmission of a data stream (e.g., MPEG-2 data) between internal components of the transceiver, in accordance with the specific type of the data. In this embodiment, the transceiver includes a first component (e.g., an A/V MPEG-2 decode block) for receiving a data stream from an external source (e.g., an MSO) and the first component includes descrambling functionality (e.g., to descramble the data stream if scrambled). A first encryption unit is coupled to the first component for encrypting the data stream to produce an encrypted data stream. The

transceiver also includes a second component (e.g., a graphics block) coupled to the first component via a bus to receive the encrypted data stream. A second encryption unit is coupled to the second component for decrypting the encrypted data stream.

As the data stream is received by the transceiver from the external source, the first encryption unit is configured to read a flag included in the data stream that indicates whether the data stream requires secure transmission. When the flag indicates that secure transmission is required, the first encryption unit encrypts the data stream and transmits via the bus the resulting encrypted data stream to the second component for further processing. When the flag indicates secure transmission is not required, the data stream is transmitted via the bus to the second component without encryption. In one embodiment, two separate memories are used to buffer the data stream prior to transmission. One memory buffers the data stream prior to encryption and subsequent transmission while the other memory buffers the data stream prior to transmission in-the-clear (e.g., when secure transmission is not required).

The encryption/decryption processes of the transceiver are coordinated and controlled by a processor included in the transceiver. The management of the encryption/decryption process causes a significant amount of processor overhead. Thus, by providing secure transmission for only those data streams which require it (e.g., copyrighted premium services), less processor cycles are consumed managing the encrypt decrypt process. This frees processor cycles for other applications, such as, for example, a richer user interface, additional user interface features, etc. In addition, less internal bus bandwidth is

occupied managing the exchange of keys required for implementing the encrypt decrypt process.

In this manner, the present invention provides a method and system that can prevent pirating of a descrambled and decrypted digital signal between multiple components (e.g., functional blocks) of an audio/video transceiver. The present invention provides a method and system to prevent pirating that can be readily implemented in a transceiver (e.g., a set-top box) used in a digital broadcast system. In addition, the method and system of the present invention prevents pirating while also reducing the overhead involved in managing the encryption-decryption process within the transceiver.

In one embodiment, the data stream from the external source is a digital audio/visual media signal delivered to the intelligent transceiver using, for example, a terrestrial line (e.g., a cable system), the World Wide Web (e.g., a connection to the Internet), or a wireless transmission (e.g., a satellite broadcast).

In one embodiment, the encrypted signal is encrypted using an encryption routine compliant with the Data Encryption Standard Electronic Code Book (DES ECB).

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

Prior Art Figure 1 is a block diagram showing some of the elements in one embodiment of a prior art transceiver (e.g., a set-top box).

Prior Art Figure 2 illustrates some of the elements in another embodiment of a prior art transceiver.

Figure 3A shows an overview diagram of a transceiver in accordance with one embodiment of the present invention.

Figure 3B shows an overview diagram depicting the relationship of the transceiver from Figure 3A to the broadcast systems available to an MSO.

Figure 4 shows a more detailed block diagram of a transceiver in accordance with one embodiment of the present invention.

Figure 5 shows a block diagram of another embodiment of a transceiver in accordance with one embodiment of the present invention.

Figure 6 shows a more detailed diagram of a transceiver showing additional details of the embodiments of Figure 4 and Figure 5.

Figure 7 shows a flow chart of the steps of a selective encryption process in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

Reference will now be made in detail to the embodiments of the invention, a method and system for selective encryption of data signals on a data bus in a transceiver, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the preferred embodiments, it will be understood that they are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the invention as defined by the appended claims. Furthermore, in the following detailed description of the present invention, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be obvious to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the present invention.

Embodiments of the present invention are directed to a method and system for selective encryption of data signals on a data bus in a transceiver. The present invention provides a method and system that can prevent pirating of a descrambled and decrypted digital signal between multiple components (e.g., functional blocks) of an audio/video transceiver. The present invention provides a method and system to prevent pirating that can be readily implemented in a transceiver (e.g., a set-top box) used in a digital broadcast system. In addition, the method and system of the present invention prevents pirating while also reducing the overhead involved in managing the

encryption/decryption process within the transceiver. The present invention and its benefits are further described below.

Notation and Nomenclature

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits within a computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as "processing" or "computing" or "transmitting" or "encrypting" or "determining" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data

represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention is described in the context of an intelligent transceiver (e.g., a set-top box) that can be used as part of a digital broadcast system. However, it is appreciated that the present invention may be utilized in other types of devices including consumer electronic devices where it may be necessary to decrypt and encrypt a digital signal.

Referring now to Figure 3A, an overview diagram of a transceiver 300 in accordance with one embodiment of the present invention is shown. Transceiver 300 includes a first component, A/V decode block 340, a second component, graphics block 350, and a CPU 360. A/V decode block 340, graphics block 350, and CPU 360 are coupled via a bus 305. In this embodiment, the A/V decode block 340 includes functionality for descrambling an incoming digital broadcast signal 370.

In accordance with the present embodiment, transceiver 300 implements a system for selective encryption of data as the data is transmitted between internal components (e.g., A/V decode block 340 and graphics block 350) of a transceiver. An incoming data stream (e.g., digital broadcast signal 370) is descrambled and decoded in A/V decode block 340 and selectively encrypted using a first encryption unit 345 before transmission via bus 305 to graphics block 350 for decryption using a second encryption unit 346.

The selective encryption provides for selectively implementing secure transmission of the data stream (e.g., MPEG-2 data) between blocks 340 and 350 of transceiver 300, in accordance with the specific type of the data. In this embodiment, transceiver 300 includes A/V decode block 340 for receiving digital broadcast signal 370 from an external source (e.g., an MSO) and descrambling the digital broadcast signal into a resulting data stream. Encryption unit 345 is included in A/V decode block 340 for encrypting the data stream from digital broadcast signal 370 to produce an encrypted data stream. Graphics block 350 is coupled to the A/V decode block 350 via bus 305 to receive the encrypted data stream. Encryption unit 346 is built into graphics block 350 for decrypting the encrypted data stream. Once decrypted, the data stream is processed by graphics block 350 to produce component audio and video signals 371 and 372 for a television 375.

The descrambling and encrypting functionality of transceiver 300 thus implements a conditional access (CA) function that allows selective access to valuable copyrighted information. Such information includes, for example, pay-per view movies, premium sporting events, etc. The producers of the movies, events, etc., require that access to the premium services be controlled in order to protect and enforce their copyrights, protect copyright ownership, and protect their commercial interests as well. Hence, the secure transmission process of the present embodiment ensures the copyrighted premium services are provided to authorized users only, thereby protecting the commercial interests of the MSOs.

Referring still to Figure 3A, as the digital broadcast signal 370 is received by the transceiver 300 from the external source, encryption unit 345 is configured to read a flag included in the digital broadcast signal that indicates whether the resulting data stream (e.g., the descrambled signal) requires secure transmission. As described above, MSOs have a commercial interest in limiting access to copyrighted premium services to authorized users only. When the flag indicates secure transmission is required (e.g., the digital broadcast signal is for a copyrighted premium service), the first encryption unit 345 encrypts the data stream and transmits via the bus the resulting encrypted data stream to the graphics block 350 for further processing. When the flag indicates secure transmission is not required (e.g., the digital broadcast signal is for standard "non-premium" service), the data stream is transmitted via the bus to graphics block 305 without encryption, thereby reducing the overhead involved in managing the encryption/decryption process within the transceiver 300.

In the present embodiment, the encryption-decryption processes of transceiver 300 are coordinated and controlled by CPU 360. In the present embodiment, CPU 360 contains a processor (not shown) for processing information and instructions. CPU 360 also may contain random access memory, read only memory, one or more caches, a flash memory and the like (not shown) for storing information and instructions. The management of the encryption/decryption process causes a significant amount of CPU overhead. Thus, by providing secure transmission for only those data streams which require it (e.g., copyrighted premium services), less CPU cycles are consumed managing the encrypt-decrypt process. This frees CPU cycles for other applications, such as, for example, a richer user interface, additional user

interface features, etc. In addition, less bandwidth of bus 305 is occupied, for example, managing the exchange of encryption keys required for implementing the encrypt-decrypt process.

Additionally, when secure transmission is required, there is not a point for intercepting a signal that is in the clear (e.g., a decrypted and descrambled signal) between A/V decode block 340 and graphics block 350. And since in the present embodiment, A/V decode block 340 and graphics block 350 are integrated circuit devices, there is no point where an in-the-clear signal can be externally accessed and intercepted.

In this manner, the transceiver 300 provides system that can prevent pirating of a descrambled and decrypted digital signal between multiple components (e.g., functional blocks) of an audio/video transceiver. Although Figure 3A depicts two such components, A/V/ decode block 340 and graphics block 350, additional components of transceiver 300 can access the data stream via bus 305 using the selective encryption process of the present embodiment. In such a case, each additional component would have its respective encryption unit (e.g., encryption unit 346) for accessing the data stream when the data stream is encrypted. Hence, as the number of components requiring access to the encrypted data stream increases, the amount of CPU overhead saved using the selective encryption process of the present embodiment increases.

With reference still to Figure 3A, as described above, a flag is included in the digital broadcast signal that indicates whether the resulting data stream requires secure transmission. This "copyright flag" is embedded within the AV

data stream itself by, for example, the MSO, prior to scrambling and modulation. Transceiver 300 receives digital broadcast signal 370 from a MSO (not shown). For example, digital broadcast signal 370 is a media signal comprising audio and video content. Digital broadcast signal 370 can be delivered to transceiver 300 using any of the various mechanisms currently in use or envisioned, such as a terrestrial line (e.g., a cable system), the World Wide Web (e.g., a connection to the Internet), or a wireless transmission (e.g., a satellite broadcast). In accordance with the present invention, a number of different digital broadcast signal formats in use or envisioned can be used, such as the Advanced Television Systems Committee (ATSC) digital television format. Which ever format or means of reception is used, the copyright flag indicates whether secure transmission is required.

The copyright flag identifies the data as being premium, copyrighted, limited access, etc. In the present embodiment, A/V decode block 340 descrambles digital broadcast signal 370 and reads the flag to determine whether the resulting data stream requires secure transmission or not. If the data requires secure transmission, the data is buffered in a first memory 373 subsequent encryption prior to transmission across bus 305 to the other components. If the data does not require secure transmission, the data is buffered in a second memory 374 for subsequent transmission in the clear across the internal bus to the other components. This data from memory 374 is not encrypted prior to transmission on bus 305.

Alternatively, as opposed to using two separate memories for buffering, a single memory can be used wherein the integrity between the data types (e.g., data requiring secure transmission and data not requiring secure

transmission) is still maintained. Integrity can be maintained through use of memory mapping schemes, separate data structures, address partitioning, or other well known memory management techniques.

Figure 3B shows an overview diagram depicting the relationship of transceiver 300 to the broadcast means of the MSO. As described above, digital broadcast signal 370 can be delivered to transceiver 300 using any of the various mechanisms currently in use or envisioned, such as a terrestrial line (e.g., a cable system), the World Wide Web (e.g., a connection to the Internet), or a wireless transmission (e.g., a satellite broadcast or terrestrial broadcast). This is depicted in Figure 3B as digital broadcast signal 370a from internet/cable 391 and digital broadcast signal 370b from satellite/terrestrial broadcast 392. Which ever format or means of reception is used, the selective encryption method of the present embodiment ensures premium copyrighted services are securely transmitted from signals 370a-370b to television 375.

Figure 4 shows a more detailed diagram of a transceiver 400 (e.g., a set-top box) in accordance with one embodiment of the present invention. In the present embodiment, transceiver 400 includes a front-end block 310 coupled to bus 305, interface card 330 coupled to front-end block 310 and bus 305, audio/video (A/V) decode block 340 coupled to interface card 330 and bus 305, graphics block 350 coupled to A/V decode block 340 and bus 305, and central processing unit 360 coupled to bus 305. Interface card 330, also referred to as a point of deployment (POD), is adapted to receive smart card 325.

Transceiver 400 of Figure 4 is substantially similar to transceiver 300 of Figure 3A. However, Transceiver 400 receives digital broadcast signal 370

via a separate front end block 310 and is transmitted to interface card 330 for descrambling and subsequent transmission to A/V decode block 340.

In the present embodiment, front-end block 310 contains one or more tuners for receiving digital broadcast signal 370. For example, in one embodiment, front-end block 310 can contain a tuner for receiving a wireless transmission (e.g., a satellite broadcast) and another tuner for receiving a cable transmission. Front-end block 310 can also include a device (e.g., a modem) that allows a telephone or digital subscriber line (DSL) connection to be made to the World Wide Web so that a broadcast signal can be received via the Internet.

Smart card 325 stores information needed by a cable system operator or digital broadcast system operator (e.g., a Multiple System Operator, MSO) in order to bill a subscriber for services used by the subscriber (for example, the viewing of a pay-per-view movie or event). Typically, smart card 325 also includes a key that is used to descramble digital broadcast signal 370 (if the signal is scrambled). In the present embodiment, smart card 325 is inserted into interface card 330; however, it is appreciated that in other embodiments smart card 325 may be coupled in a different manner to intelligent transceiver 300 (for example, it may be inserted into either front-end block 310 or A/V decode block 340). Using the key from smart card 325, interface card 330 descrambles digital broadcast signal 370.

In the present embodiment, interface card 330 includes buffers 473-474 which function in a manner similar to buffers 373-374 of Figure 3A. Interface card 330 descrambles digital broadcast signal 370 and reads the flag to

determine whether the resulting data stream requires secure transmission or not. If the data requires secure transmission, the data is buffered in a first memory 473 subsequent encryption. If the data does not require secure transmission, the data is buffered in a second memory 474 for subsequent transmission in the clear.

Because digital broadcast signal 370 has been descrambled, when secure transmission is required, the signal must be encrypted in order to prevent its unauthorized use and duplication. In the present embodiment, interface card 330 contains an encryption unit (not shown) that encrypts digital broadcast signal 370. In one embodiment, the encryption unit uses a well-known DES ECB (Data Encryption Standard Electronic Code Book) encryption routine and a key length of 56 bits. However, it is appreciated that other well-known and commercially available encryption routines and different key lengths may be used in accordance with the present invention.

In the present embodiment, A/V decode block 340 is an integrated circuit device comprising a functional block and a encryption unit 345 integrated therein. Encryption unit 345 is integral with A/V decode block 340 (that is, as a single integrated circuit, or "chip") and coupled to front-end block 310 via interface card 330. In this embodiment, the link between interface card 330 and A/V decode block 340 (specifically, encryption unit 345) is separate from bus 305; that is, there is a direct connection between interface card 330 and encryption unit 345 that bypasses bus 305.

Encryption unit 345 decrypts an encrypted signal (e.g., digital broadcast signal 370) received by A/V decode block 340. The output of encryption unit

345 is a decrypted digital signal that is "in the clear." The signal in the clear is transmitted within A/V decode block 340 for decoding. When secure transmission is required (as indicated by the copyright flag described above), the clear signal is encrypted by encryption unit 345 prior to transmission outside of A/V decode block 340.

Thus, when secure transmission is required, there is not a point for intercepting a signal that is in the clear (e.g., a decrypted and descrambled signal) between interface card 330 and encryption unit 345, nor is there a point between encryption unit 345 and A/V decode block 340 where an in-the-clear signal can be externally accessed and intercepted. Therefore, the present invention provides a secure interface between interface card 330 and encryption unit 345 and also between encryption unit 345 and A/V decode block 340, and thus between front-end block 310 and A/V decode block 340. As such, the present invention can prevent pirating of a descrambled and decrypted digital signal. However, when secure transmission is not required, the in-the-clear signal is transmitted between interface card 330, A/V decode block 340, and graphics block 350.

In the present embodiment, when secure transmission is required, A/V decode block 340 receives encrypted digital broadcast signal 370 from interface card 330, decrypts the signal using encryption unit 345, and decodes the video content and the audio content of digital broadcast signal 370. In the present embodiment, an MPEG (Moving Pictures Experts Group) video decoder and an AC3 (Digital Dolby) audio decoder are used; however, it is appreciated that other video or audio decoders can be used in accordance with the present

invention. In addition, in one embodiment, A/V decode block 340 is capable of handling video and audio analog signals.

Figure 5 is a block diagram of a transceiver 500 in accordance with another embodiment of the present invention. In this embodiment, point of deployment (POD) 320 is separate from interface card 330, and smart card 325 is plugged into POD 320 instead of interface card 330. Selective encryption in accordance with the copyright flag embedded in digital broadcast signal 370 is still implemented in interface card 330 in the manner described above. In this embodiment, however, smart card 325 contains a key for descrambling digital broadcast signal 370, and this key is used by POD 320 to descramble digital broadcast signal 370. POD 320 also encrypts digital broadcast signal 370 using an encryption engine (not shown). Although POD 320 is separate from interface card 330 in this embodiment, interface card 330 can still exist in intelligent transceiver 500.

Figure 6 is a block diagram of a transceiver 600 (e.g., a bi-directional set-top box) showing additional details of the embodiments illustrated by Figure 4 and Figure 5. Table 1 is a list of the various elements and acronyms contained in Figure 6.

Table 1

Elements and Acronyms of Transceiver Embodied in Figure 6

AVDAC	Audio Video Digital-to-Analog Converter
BTSC	Broadcast Television Systems Committee
D-Cache	Data Cache

DAVIC	Digital Audio Visual Council
DOCSIS	Data Over Cable Service Interface Specification
DSM	Diplexer, Splitter and Modulator
DSP	Digital Signal Processor
DVD	Digital Video Disk
FAT	Forward Application Tuner
FPU	Floating Point Unit
I/F	Interface
IDCT	Inverse Discrete Cosine Transform
Inst. Cache	Instruction Cache
Int. Cont.	Interrupt Controller
MAC	Media Access Control
MC	Motion Compensation
MCNS	Multiple Cable Network System
MIDI	Musical Instrument Digital Interface
MP@ML	Main Profile at Main Level
OOB	Out of Band
PCI	Peripheral Component Interconnect
PCM	Pulse Code Modulation
PLL	Phase Locked Loop
QPSK	Quadrature Phase Shift Keying
QPSKQAM	QPSK Quadrature Amplitude Modulation
RTC	Real Time Clock

SLIC	Serial Line Internet Connection
UART	Universal Asynchronous Receiver-Transmitter
VBI	Vertical Blanking Interval
VIF/SIF	Video Intermediate Frequency/Sound Intermediate Frequency

With reference to Figure 6, in the present embodiment, front-end block 310 receives a scrambled digital broadcast signal (e.g., digital broadcast signal 370 of Figures 3A and 3B) from a digital broadcaster via in-band tuner 401, OOB tuner 402 and/or MCNS FAT tuner 403. Smart card 325 includes a key to descramble the digital broadcast signal. It is appreciated that Figure 4 shows some elements from the embodiments illustrated by Figures 3, 4, and 5. In the case of the embodiment illustrated by Figure 4, smart card 325 is inserted into interface card 330, and interface card 330 descrambles and encrypts the digital broadcast signal. In the case of the embodiment illustrated by Figure 5, smart card 325 is plugged into POD 320. In this latter embodiment, the descrambling and encrypting functions are performed in POD 320, and so these functions are bypassed in interface card 330. In the case of the embodiment illustrated by Figure 3A, the separate buffers 373 and 374 are included in block 340 for the encrypted data stream and non-encrypted data stream.

Continuing with reference to Figure 6, when encryption is required, the encrypted digital signal is delivered to A/V decode block 340 via interface card 330. In the present embodiment of the present invention, decryption engine 345 is integrated into demultiplexer ("demux") 410, which is itself integrated into A/V decode block 340. Decryption engine 345 contains an decryption

engine for decrypting digital broadcast signal 370. Decryption engine 345 is integral with A/V decode block 340 and is coupled to front-end block 310 via interface card 330. Decryption engine 345 decrypts an encrypted signal (e.g., digital broadcast signal 370) received by A/V decode block 340 via interface card 330. The in-the-clear signal is immediately transmitted within the integrated circuit of A/V decode block 340 for decoding. Thus, as described above, when secure transmission is required, the in-the-clear signal is not transmitted outside the physical block comprising A/V decode block 340 and decryption engine 345. In the present embodiment, decryption engine 345 provides the interface between A/V decode block 340 and interface card 330. It is appreciated that in other embodiments integrated circuit 345 may be integrated into A/V decode block 340 in some different manner (that is, in a location other than demux 410) while still providing the interface with interface card 330.

As explained above, when secure transmission is not required (as indicated by the flag included in the digital broadcast signal 370) the descrambled data stream is transmitted as an in-the-clear signal (e.g., descrambled and not encrypted) between interface card 330 and block 340, and between block 340 and block 350. When secure transmission is required, the descrambled data stream is first encrypted by interface card 330 prior to transmission to block 340, and encrypted by encryption unit 345 prior to transmission to block 350, such that the descrambled data stream is not exposed as an in-the-clear signal (e.g., descrambled and not encrypted) between interface card 330, block 340, and block 350. Therefore, the selective encryption process of the present invention provides a secure interface between interface card 330 and decryption engine 345 and between decryption

engine 345 and A/V decode block 340, and thus between front-end block 310 and A/V decode block 340 on an as-needed basis, thereby reducing overhead on CPU 360.

Continuing with reference to Figure 6, in the present embodiment, A/V decode block 340 includes an MPEG decoder (e.g., graphics block 411) and an audio decoder (e.g., AC-3 block 412) to decode the video and audio content of digital broadcast signal 370. Graphics block 350 processes the audio and video information received from A/V decode block 340. Central processing unit 360 contains a processor (e.g., CPU core 430) and memory (e.g., instruction cache 420) for processing information and instructions used by intelligent transceiver 400.

Referring now to Figure 7, a flow chart of the steps of a process 700 in accordance with one embodiment of the present invention is shown. Process 700 depicts the basic operating steps of a selective encryption process as implemented in a set-top box transceiver in accordance with one embodiment of the present invention (e.g., transceiver 300 of Figure 3A).

Process 700 begins in step 701, where a digital broadcast signal is received by transceiver 300. As described above, the digital broadcast signal is transmitted from an MSO. The digital broadcast signal (e.g., digital broadcast signal 370 of Figure 3A) includes a copyright flag that indicates whether the digital broadcast signal is, for example, a copyrighted premium service.

In step 702, the digital broadcast signal is descrambled using descrambling circuits. As described above, the digital broadcast signal is

transmitted from the MSO in a scrambled form to prevent unauthorized reception by "pirating" users. An authorized user can descramble the digital broadcast signal using a key provided by the MSO. Depending upon the particular transceiver embodiment, the descrambling functionality can be included in an A/V decode block (e.g., transceiver 300 of Figure 3A), or a separate interface card (e.g., interface card 330 of Figure 4).

In step 703, the copyright flag in the descrambled data stream is read to determine whether secure transmission of the data stream is required. As described above, this flag indicates, for example, whether the digital broadcast signal is a copyrighted premium service. Depending upon the particular transceiver embodiment, the copyright flag can be read in an A/V decode block or a separate interface card.

Referring still to process 700 of Figure 7, in step 704, if the copyright flag read in step 703 indicates secure transmission is required, process 700 proceeds to step 707, where the descrambled data stream is encrypted prior to transmission. If the copyright flag indicates secure transmission is not required, process 700 proceeds to step 705, where the descrambled data stream is transmitted among the internal components of the transceiver in the clear.

In step 705, where secure transmission is not required as determined in step 704, the descrambled data stream is buffered in a first memory (e.g., memory 374 of Figure 3A). As described above, the data is buffered in the memory buffer for subsequent transmission in the clear across the internal

bus to the other components. This data is not encrypted prior to transmission on the bus.

In step 706, the data stored in the memory buffer from step 705 is transmitted in the clear from, for example, the A/V decode block 340 to the graphics block 350 across the bus.

In step 707, where secure transmission is required as determined in step 704, the descrambled data stream is buffered in a second memory (e.g., memory 373 of Figure 3A). This data is encrypted prior to transmission. Alternatively, as opposed to using two separate memories for buffering, a single memory can be used wherein the integrity between the data types (e.g., data requiring secure transmission and data not requiring secure transmission) is still maintained. As described above, integrity can be maintained through use of memory mapping schemes, separate data structures, address partitioning, or other well known memory management techniques.

In step 708, encryption/decryption keys are distributed by a CPU included in the transceiver (e.g., CPU 360 of Figure 3A) to each encryption unit of the components of the transceiver. As described above, to prevent access to an in-the-clear signal, the descrambled data stream is encrypted prior to transmission from, for example, A/V decode block 340 to graphics block 350. The encryption process (e.g., a well-known DES ECB encryption routine and a key lengths of 56 bits) is managed and coordinated by the CPU. The distributed encryption keys allow each encryption unit (e.g., encryption units 345-346) to encrypt and/or decrypt the data stream as needed.

In step 709, the descramble data stream is encrypted prior to transmission across the internal busses of the transceiver. As described above, prior to transmission from each component or block, the data stream is encrypted to prevent any point of access for pirating the signal. Hence, when secure transmission is required, the descrambled data stream is not exposed outside any of the components or blocks of the transceiver.

Thus, the present invention provides a method and system for selective encryption of data signals on a data bus in a transceiver. The present invention provides a method and system that can prevent pirating of a descrambled and decrypted digital signal between multiple components (e.g., functional blocks) of an audio/video transceiver. The present invention provides a method and system to prevent pirating that can be readily implemented in a transceiver (e.g., a set-top box) used in a digital broadcast system. In addition, the method and system of the present invention prevents pirating while also reducing the overhead involved in managing the encryption/decryption process within the transceiver.

The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application. It is intended that the scope of the invention be defined by the Claims appended hereto and their equivalents.

CLAIMS

What is claimed is:

1. A system comprising:

a first component of a transceiver for receiving a data stream;

a first encryption unit associated with the first component for encrypting the data stream to produce an encrypted data stream;

a second component of the transceiver coupled to the first component via a bus and for receiving the encrypted data stream;

a second encryption unit associated with the second component and for decrypting the encrypted data stream; and

the first encryption unit configured to read a flag included in the data stream, the flag indicating whether the data stream requires secure transmission, wherein the first encryption unit encrypts the data stream provided the flag indicates that secure transmission is required.

2. The system of Claim 1 wherein the first encryption unit is coupled to the first component, the second encryption unit is coupled to the second component, and the first encryption unit transmits the data stream without encryption provided the flag indicates that secure transmission in not required

3. The system of Claim 1, wherein:

the data stream being from a digital broadcast signal;

a first encryption unit being within the first component, the first encryption unit further configured to transmit an unencrypted data stream

provided the flag indicates secure transmission is not required;

a second component of the transceiver coupled to the first component via the bus for receiving the unencrypted data stream; and

a second encryption unit being within the second component, the second encryption unit for decrypting the encrypted data stream such that the unencrypted data stream is not exposed on the bus when secure transmission is required and reducing overhead from the first encryption unit and the second encryption unit when secure transmission is not required.

4. A method comprising the steps of

a) receiving a signal from an external source using a first component of a transceiver;

b) generating a data stream by descrambling the signal using the first component;

c) determining whether the data stream requires secure transmission by reading a flag included in the data stream wherein the flag is read by the first component;

d) if the flag indicates secure transmission is required, encrypting the data stream using a first encryption unit to generate an encrypted data stream and transmitting the encrypted data stream to a second component via a bus wherein the second component uses a second encryption unit to receive the encrypted data stream; and

e) if the flag indicates secure transmission is not required, transmitting an